☑ Original ☐

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Five Twitter accounts, stored at premises owned, maintained, controlled, or operated by X Corp; See Attachments

Case No. 23-M-487 (SCD)

Matter No.: 2023R00139

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A; over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12-18-23 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 12-4-23. 9:50 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with Twitter accounts:

- "@bellamellayella", account #717375314483967;
- "@lexxiisback", account #111100982120124416;
- "@_LoveEndia", account #2755568626;
- "@BiSexUWell", account #1017895112729296896; and
- "@X.aldn", account #1711486293023059968,

(the "Accounts") that are stored at premises owned, maintained, controlled, or operated by X Corp., a company headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by X Corp.

To the extent that the information described in Attachment A is within the possession, custody, or control of X Corp., regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to X Corp., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 17, 2023 (Case #0348939677), X Corp. is required to disclose to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from June 1, 2021 to present;

7. Privacy and account settings, including change history; and

8. Communications between X. Corp. and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the Account from June 1, 2021 to present, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the Account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the Account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the Account and other Twitter users from June 1, 2021 to present, including but not limited to:

1. All users the Account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the Account;

2. All information from the "Connect" or “Notifications” tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., “mentions” or “replies”);

3. All contacts and related sync information; and

4. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the Account, including but not limited to:

1. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the Account;

3. All records of searches performed by the from June 1, 2021 to present;

4. All location information, including all location data collected by any plugins, widgets, or the “Tweet With Location” service, from from June 1, 2021 to present; and

5. All information about the Account's use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the Account was clicked.

X Corp. is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C § 2252(3)(A) and 2252(3)(B) – Knowlingly sell or possess with intent to sell Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1) – Transportation of Child Pornography and 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2) – Possession of Child Pornography, those violations involving Endia Taper and unknown subjects and occurring after June 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The receipt, sale, transportation, or possession on Child Sexual Abuse Material;

(b) Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account owner;

(c) Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic

data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Five Twitter accounts, stored at premises owned, maintained, controlled, or operated by X Corp; See Attachments

Case No. 23-M-487 (SCD)

Matter No.: 2023R00139

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A; over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 371; 922(a)(6); and 924(a)(1)(A)	Possession or sale of firearms; Evidence of straw purchasing firearms and illegal firearms trafficking;

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Daniel Gartland, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 12-4-23

Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

Matter No.: 2023R00139

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Twitter accounts that are stored at premises owned, maintained, controlled, or operated by X Corp., an electronic communications service and/or remote computing service provider headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require X Corp. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate

violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as "CSAM").

4. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 2252(3)(A) and 2252(3)(B) – Knowlingly sell or possess with intent to sell Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1) – Transportation of Child Pornography and 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2) – Possession of Child Pornography have been committed by Endia Taper (XX/XX/1998). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

DEFINITIONS

7. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B (collectively referred to as "warrant"):

a. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in

sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); United States v. Riccardi, 258 F.Supp.2d 1212 (D. Kan., 2003) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

f. "Electronic device" includes any electronic, magnetic, optical, electrochemical or other high speed system or device capable of storing and/or processing data in digital form, including but not limited to the following: central processing units; desktop, laptop, and notebook computers; tablets; PDAs; wireless communication devices such as cellular telephones and pagers; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, routers, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, flash drives, magnetic tapes and memory chips; security devices; and any data storage facility or communications facility directly related to or operating in conjunction with such device.

g. "Hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to hardware (including physical keys and locks).

h. "Software" is digital information which can be interpreted by an electronic device and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Electronics-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use hardware, software, or other related items.

j. "Passwords and data security components" consist of information or items designed to restrict access to or hide software, documentation, or data. Data security components may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters or symbols) usually operates a sort of digital key to "unlock" data security components. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "Internet Service Providers" (ISPs) are commercial organizations, which provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means to access the internet, including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, fiber optic cable, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox. The subscriber is then typically required to create a password for the account. By using an internet-capable electronic device, the subscriber and other users can establish digital communication with an ISP and thereby access the internet.

l. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

m. "Internet Protocol address" (IP address) refers to a unique number used by an electronic device to access the internet. IP addresses can be dynamic, meaning the Internet Service Provider (ISP) assigns a different unique number to an electronic device every time it accesses the internet. IP addresses are considered static if an ISP assigns a user's electronic device a particular IP address, which is used each time the device accesses the internet.

n. The terms "records," "documents" and "materials" include all information recorded in any form, visual or audio, and by any means, whether in hand-made form (including writings, drawings, painting); photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including phonograph records, printing, typing); or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators; and digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but certain attributes may change during the reproduction.

p. "Log Files" are records automatically produced by software to document electronic events that occur on electronic devices. Software can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote electronic devices; access logs list specific information about when an electronic device was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

q. "Cellular telephones" are handheld electronic devices used for wireless voice and data communication through radio signals. These telephones send signals through

networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Emojis" are small digital images or icons used in electronic messages or webpages to communicate an idea, emotion, expression, or feeling. Emojis exist in various genres, including facial expressions, common objects, places, types of weather, and animals.

BACKGROUND ON ELECTRONIC DEVICE USE IN FACILITATING CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION CRIMES

8. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Electronic devices and related technology have revolutionized the way in which child pornography is produced, distributed, viewed, and stored, as well as how it is used in furtherance of online child exploitation.

b. Individuals can convert photographs and videos taken using a traditional camera or video recorder to a format capable of being disseminated quickly and efficiently via the internet using a variety of electronic devices, including scanners, memory card readers, cellular telephones, or directly from digital cameras.

c. Modems and routers allow electronic devices to connect to other devices using telephone, cable, or wireless connections. Electronic contact can be made to literally millions of devices around the world.

d. The capability of electronic devices to store extremely large amounts of high-resolution video and imagery in digital form, which can be password protected or hidden from other device users, makes these devices highly effective at storing child pornography, while also concealing the user's illicit activity.

e. The internet affords individuals many different and relatively secure and anonymous venues for obtaining, viewing, and distributing child pornography; or for communicating with others to do so; or to entice children.

f. Individuals can use online resources to retrieve, store and share child pornography, including services offered by internet portals such as Google, Yahoo!, and Facebook, among others. Online services, which are accessed via electronic device, generally allow a user to set up an account which thereby provides the user with access to email, instant messaging services, online file storage, social media, online message boards, and/or a variety of other interconnected web-based applications. If a user uses any of these functions to obtain, view, store, or distribute child pornography; or for communicating with others to do so; or to entice children, evidence of such activity can often be found on the user's electronic device.

g. As is the case with most digital technology, electronic device communications can be saved or stored on hardware and digital storage media. Storing this information can be intentional, i.e., by saving an e-mail as a file on the electronic device or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic device user's internet activity generally leaves traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

h. The interaction between software and the electronic device's operating systems often results in material obtained from the internet being stored multiple times, and even in different locations in the device's digital memory, without the user's knowledge. Even if the device user is sophisticated and understands this automatic storage of information, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the digital media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's digital media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution, and/or possession of child pornography.

i. Data that exists on an electronic device is particularly resilient to deletion. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on most electronic devices, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space

or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user's operating system, storage capacity, and device habits.

CHARACTERISTICS OF INDIVIDUALS INVOLVED IN THE DISTRIBUTION OF CHILD PORNOGRAPHY

9. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the possession and distribution of child pornography. Those who possess and distribute child pornography:

a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, electronic storage media, or other visual media. Such individuals often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Often possess and maintain their "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., within their residences, attached or detached garages, associated outbuildings, their vehicles, and/or other secure locations which they maintain dominion and control of, for ready access and to conceal these items from law enforcement, family members, or other individuals who frequent these areas. These individuals typically retain pictures, films,

photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, videotapes, and electronic storage media for many years.

d. Often maintain their digital or electronic child pornography collections in a safe, secure, and private environment, such as on an electronic device. These collections are highly valued by the individual, are often maintained for several years, and are kept close by, usually within their residences, attached or detached garages, associated outbuildings, their vehicles, and/or other secure locations which they maintain dominion and control of, for ready access and to conceal these items from law enforcement, family members, or other individuals who frequent these areas.

e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated."

PROBABLE CAUSE

11. On October 26, 2023, a Special Agent with the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), contacted the FBI regarding a cellular telephone that was suspected to contain Child Sexual Abuse Material (CSAM). The phone, an Apple iPhone 12 with serial number "GT2LHW2MX2" (hereinafter, "iPhone 12"), was seized during a residential search warrant executed by the ATF on October 20, 2023. Endia Taper claimed ownership of the iPhone 12 and provided the passcode to access the phone during an interview with an ATF agent at the

residence.

12. The ATF conducted a forensic download of the iPhone 12, pursuant to a search warrant for evidence of violations of federal firearms laws. While conducting a review of the forensic download of the iPhone 12, an investigator observed two videos which were suspected to be Child Sexual Abuse Material, at which time the review of the device ceased. The following information was extracted from the device during the forensic download:

- Accounts: endiamarie0@gmail.com; endiamariee@icloud.com
- Owner name: Endia Taper
- Model: iPhone 12
- Serial number: GT2LHW2MX2
- Phone number: 1-414-712-2975
- IMEI: 354696402450909
- IMEI(2): 354696402061920

13. I observed portions of the suspected CSAM videos two of which are further described as follows:

- A video depicting a nude, prepubescent female. The child was visible from below the sternum to her legs. The child lacked pubic hair and had a body size and lack of muscular development consistent with the approximate age range of 4 to 9 years old. Her vagina was exposed and legs spread. She appeared to be laying on her back. An erect penis rubbed on the child's vagina without penetration and ejaculated onto the child's vagina. The video appeared to be a compilation of multiple videos of the same style, as the video continued to show another incident of child sexual abuse.

- A video depicting a close-up of the faces of two Asian males. The facial features of the boys were consistent with approximate ages under 10 years old. An erect penis was visible between the children's faces. The boy's were orally penetrated by the erect penis.

14. A search of law enforcement databases revealed that in Endia Taper was associated with telephone number 414-712-2975 since approximately March 2021.

15. On October 30, 2023, Endia Taper was interviewed at the ATF offices in Milwaukee, WI. Taper confirmed she was the only person with access to the iPhone 12 and it was typically in her possession. Taper maintained a Twitter and Telegram accounts on the iPhone 12. She used the account to sell pictures of her breasts and videos of herself dancing. Taper used the applications because she did not want her customers to know her phone number or any of her personal information.

16. Taper had received images of child pornography from Telegram users. The images were unsolicited. Taper deleted the images when they were received. Taper did not seek out child pornography and was not sexually attracted to children. Taper believed that she was sent the images because she engaged in video calls with her customers, during which she acted out incest fantasies with them.

17. On October 30, 2023, a search warrant, issued in the United Stes District Court for the Eastern District of Wisconsin was executed on the iPhone 12. The device and a forensic download of the device were provided to the FBI. A manual review of the device was conducted on November 1, 2023.

Telegram

18. The Telegram application was observed to be installed on the iPhone 12 and was

locked with the same pin used to lock the phone. The identifier lexiixoxo09 was associated with the application along with telephone number 414-712-2975. The application appeared to have 1.8 GB capacity of cloud storage. Approximately 1.4 GB of the cloud storage was allocated to videos. The cloud storage could not be accessed during the review, as the device was disconnected from wireless and cellular networks.

19. A review of the forensic download of the device was initiated on November 13, 2023. Conversations and images associated with the Telegram account were recovered from the device. 307 videos were recovered with file names that included "telegram-cloud-document" in the naming convention. Over 250 of those videos were determined to be CSAM. Four of those videos are described as follows:

- A video taken from the perspective of a male with an erect penis in his hand. A crying infant laying in a bed with a white sheet was visible infront of the male. The infant was wearing only a diaper. The male moved closer to the infant and inserted his erect penis into the infant's open mouth repeatedly. The male appeared to ejaculate into the infant's mouth and onto the infant's face. The video was last accessed on the device on September 28, 2023 at 6:51 PM UTC. The file name included "telegram-cloud-document."
- A video taken from the perspective of a black male with an erect penis. A black child of undetermined sex was laying on a white sheet with a floral pattern, partially covered with a blanket. The child's physical size and lack of musculature were consistent with the approximate age range of 4 to 9 years old. The child was wearing a white T-shirt and bright green bottoms. The child appeared to be partially asleep and its hand was gripping the male's erect penis. The male moved

his hips in an apparent effort to cause the child to manipulate his penis, then grabbed the child's wrist and forced the child to manipulate the penis. Another child's foot was also visible in the video. The video was last accessed on September 30, 2023 at 4:47 PM UTC. The file name included "telegram-cloud-document."

- A video taken from the perspective of a black male with an erect penis. A black female child was visible, facing away from the camera on a bed. The child's size and physical development were consistent with an age of approximately 1 to 3 years old. The child was on her hands and knees with her head resting on the bed with pink and blue covering. The child's light blue dress was pulled up to her back and her diaper was pulled down, exposing her buttocks. The male pushed is erect penis against the child's anus. The video was last accessed on September 28, 2023 at 1:43 PM UTC. The file name included "telegram-cloud-document."
- A video taken from the perspective of an adult white male. The video depicts a white female child with her legs held up in one hand by the adult male. The child lacked pubic hair and had physical development consistent with an approximate age range of 1 to 3 years old. The child was wearing a red t-shirt and was nude from the waist down. Her vagina was fully visible. The adult male's erect penis anally forcefully penetrated the child repeatedly throughout the video. When the male extracted his penis, a white substance consistent with ejaculate was visible in near the child's anus. The video was last accessed September 28, 2023. The file name included "telegram-cloud-document."

20. The following conversation between the user of the phone and an unknown

Telegram user took place on October 18, 2023:

> Lexii Xoxo (user of the iPhone 12): yeah i dobut i like to talk to ppl who can atleast spend 10 even if it s for sexting or whatever thanks for understanding
> Unknown: ahhh ok i thought you was a just taboo person that wanted to find other likeminded ppl to talk and vibe with i don t want to waste your time i know you just want to talk to ppl who are going to buy content
>
> Unknown: do your thing and enjoy your day
>
> Unknown: i appreciate it though
>
> Unknown: are you mostly content seller
>
> Unknown: of course I know you hustling
>
> Lexii Xoxo: yes

21. Based upon my training and experience, I know the term "taboo" to reference sexual material or topics, both legal and illegal, that are generally not widely accepted in society. Child Sexual Abuse Material (CSAM) could be categorized as taboo among possessors and distributors of CSAM. The term taboo could also be used by such individuals as a guise in conversations to mask their true meaning from unknowing parties or law enforcement.

22. The following conversation between the user of the phone and user "Real Ghost" took place via the Telegram application on October 20, 2023:

> Lexii Xoxo: Hey
>
> Real Ghost: Hey
>
> Lexii Xoxo: What u been up to?
>
> Real Ghost: Training all week, on Twitter chillin lol not making captions or anything just got a private page liking shit
>
> Lexii Xoxo: lol right I been trying not to go to crazy on there
>
> Real Ghost: Wyd
>
> Lexii Xoxo: nun horny asf ian been on no pervy shit ina minute but im craving it rn

Real Ghost: I don't like it when you don't hit me up for a while then ask for shit lmao
Real Ghost: Anybody for that matter but especially you cause we tight lol plus you be tryn charge me for shit when I ask you to look out

Real Ghost: [Expiring video sent]

Real Ghost: This me

Lexii Xoxo: Ion need nun from u lol I just wanted to chat honestly

Lexii Xoxo: and let me see again it went to fast

Real Ghost: Because I don't need nobody screen shooting my shit

Lexii Xoxo: U know I'm not gone do that

Real Ghost: [Expiring video sent]

Real Ghost: Regardless

Lexii Xoxo: who is the lg

Lexii Xoxo: shit sexy asf

Real Ghost: My daughter

23. The user of the phones' statement, "nun horny asf Ian been on no pervy shit ina minute but im craving it rn" indicated the conversation was intended to be sexual. Real Ghost's responses further indicate that the users trade sexual material and the user of the phone has attempted to charge Real Ghost for the material in the past.

24. A manual review of the iPhone 12 revealed that during the above conversation, Real Ghost sent two videos to the user of the phone at 1:47:24 PM UTC and 1:48:24 PM UTC. Based upon the context of the conversation, Real Ghost sent the same video twice. Two videos with the same timestamps as the conversation and depicting the same imagery were recovered from the forensice download of the telephone. The videos are further described as follows:

- A video depicting a close-up view of a black male's erect penis and the buttocks

of a black individual of an unknown sex. The erect penis was partially inserted into the buttocks. The image could not be classified as CSAM, as the age of the individual could not be reliably approximated based upon what was visible of the person. The file was last accessed on October 20, 2023 at 1:48 PM UTC. The file name included "telegram-cloud-document."

25. Based upon my training and experience, I believe the user of the phone's term "lg" to be an abbreviation for "little girl." I believe the term was used to infer a young age upon the individual of an unknown sex in the video. This belief is supported by Real Ghost's response of, "My daughter." Based upon the sexual context of the conversation and descriptive references to the videos, I believe the user of the phone and Real Ghost have traded CSAM in prior unrecovered interactions.

26. On October 20, 2023, the user of the telephone initiated a conversation with user "Hundo" via the Telegram application. During the conversation, the user of the telephone asked, "got some vids? I lost them all." The conversation concluded without a response from "Hundo".

27. On October 20, 2023, user "Meme 321" initiated a conversation with the user of the phone via Telegram. The conversation was as follows:

Meme 321: Send some [pizza slice emoji]

Lexii Xoxo: U send me some tf

Meme 321: I will I have links

Meme 321: Trds

Meme 321: I first tho like I said

28. Based upon my training and experience, I know "pizza," "za" and "homemade pizza" are terms commonly used to refer to CSAM by individuals that trade the material. I further

know that CSAM is often traded via links to cloud storage services, such as Mega Links or DropBox. Traders of CSAM will often request users send an image before trading all of their material in an attempt to identify law enforcement.

29. On October 20, 2023, user "Not Important" initiated a conversation with the user of the phone via the Telegram application at 1:41 PM UTC. User "Not Important" sent 12 videos of CSAM without and greeting or prompt to begin the conversation, then stated, "This all I got." The user of the phone responded, "Ok fina send some stuff I have," followed by a squirting emoji. The conversation concluded at 1:42 PM UTC and was subsequently deleted. One of the videos is described as follows:

- A video focused on the nude groin of a dark skinned male infant. The infant was laying on a white blanket with a yellow and green pattern. The hand of an adult of unknown sex manipulated the infant's penis with their thumb and forefinger. The adult had nail extensions. The video was last accessed on October 20, 2023 at 1:43 PM UTC. The file name included "telegram-cloud-document."

30. Based upon my training and experience, I know the Telegram application is commonly used by individuals seeking to trade or obtain CSAM. Users of the application know ownership of the application is based outside of the United States and is not responsive to legal process from the United States. The Telegram privacy policy states they will only respond to a court order that confirms a user is a terror suspect. The servers that support the application are physically located outside of the United States. These factors provide users with comfort that illegal activities, including the trade of CSAM, will not be observed by law enforcement in the United States.

Twitter

31. The X application, formerly known as Twitter was observed to be installed on the device. Multiple Twitter accounts were associated with the device, including the following:

- Account: **@lexxiisback;** display name: **Lexxii, account #1711100982120124416**
- Account: **@_LoveEndia, account #2755568626**
- Account: **@bellamellayella, account #1141847693251268609**

32. The searched items log recovered during the forensic download of the iPhone 12 revealed that the term "trade on tele" was searched in the Twitter application on an undetermined date.

33. Conversations associated with the Twitter accounts were recovered during the forensic download of the iPhone 12. On October 19, 2023, Twitter user "**X.Aldn**" initiated a conversation with the **@lexxiisback** account. The user of the phone stated, "Hey, I got homemade pizza for sale." User "**X.Aldn**" responded, "I don't buy, sorry." The conversation then concluded without any exchange of images. Based upon my training and experience, I believe the user of the phone was attempting to sell CSAM.

34. The following conversation between the user of the phone and Twitter user "**BiSexUWell**" took place on October 20, 2023:

Lexxii (user of the iPhone 12): Wanna trade one tele?

BiSexUWell: We can I just don't have that much vids cuz I had to make a new account

Lexxii: Ok lexiixoxo9 is my tele u start. I got plenty vids I just like trading for the fuck of it lol

35. The conversation concluded at 1:38 PM UTC. The Telegram conversation in which user "Not Important" sent 12 videos of CSAM was initiated less than 3 minutes later. I believe the the conversations with Twitter user "**BiSexUWell**" and Telegram user "Not Important" reflect the

user of the phone's method of obtaining CSAM. The user of the phone identified individuals with a mutal interest in trading CSAM via Twitter and traded CSAM via the Telegram application to avoid law enforcement detection.

36. On December 11, 2021, the National Center for Missing and Exploited Children created CyberTipline report #110447170. The report was initiated due to an anonymous complaint regarding Twitter account **@bellamellayella**. The report alleged the account was associated with child pornography, though further information could not be obtained to confirm the allegation. The report provided a link the the account profile page, which indicated the account was suspended due to a violation of rules.

37. Two notification emails from Twitter were recovered from the forensic download of the iPhone 12. The emails appear to notify a Twitter user of a message sent to their account, including the text of the message. A notification email from Twitter to bellaabadd12@gmail.com indicated Twitter user @DreamCodein sent a direct message. The text of the email stated, "It's murkyperc from wickr I still haven't been added to the group for the $20 I sent." The email was dated June 10, 2023.

38. A notification email from Twitter to ashantiid0@gmail.com indicated Twitter user @Matthewsep25, display name "home of taboo", sent a direct message. The text of the email stated, "I love young ass pussy I'll do anything to rape that tight hole." The email was dated September 8, 2023.

Other pertinent information

39. A note created on June 24, 2023 was recovered during the forensic download of the iPhone 12. The note was titled, "menu for lexi [water squirt emoji][two heart emoji][pizza slice emoji]." The text of the note was as follows:

facetimes-$40
phone calls-$30
sexting-$15
private snap story-$15
taboo group entry-$10
videos - $50 for 10 (bundle deal) one vid is $30.
custom vid- price varies on what u want to see me do. *i do everything no limits!
nudes-$5 each
ASK FOR ANYTHING YOU DON'T SEE ABOVE!
NO PREVIEWS! only reviews
method of payment- prefer PAY PAL! also takes Venmo or cash app as a second option.

40. Based upon my training and experience, the note represented a draft price list of sexual related services the user of the phone intended to sell. Based upon the inclusion of a pizza slice emoji with the video line item, I believe the user of the phone intended to sell CSAM.

41. The CashApp account with display name Pretty was associated with iPhone 12. Transactions for the account were recovered during the forensic download of the device. Certain transactions were consistent with the price list observed on the phone, including the following:

- June 10, 2023, user "Vic" sent $50, description: "Kilo_02 On Tele", status: canceled
- July 23, 2023, user "Commonman22" sent $60, description: "bella", status: completed
- July 27, 2023, user "Commonman22" sent $1, description: "can you sent me the files?", status: completed
- August 5, 2023, user "Commonman22" sent $40, description: "Boomboo22", status: completed
- August 5, 2023, user "Commonman22" sent $20, description: none, status: completed

42. The username "Boomboo22" was saved to the contacts on the phone and associated

with the Wickr communication application. On October 20, 2023, the user of the phone initiated a conversation with "Boomboo22" via the Wickr application, stating "Hey [squirting emoji]." The Wickr username associated with the phone was "bellafreak1". Based upon my training and experience, I believe the user of the phone identifies customer on multiple different communication applications and attempts to sell sexual material, including CSAM.

43. Based upon the provided information, there is probable cause to believe the users of the SUBJECT ACCOUNTS have received, transported, or possessed images of Child Sexual Abuse Material. There is probable cause to believe that evidence of those violations of federal law will be found in the SUBJECT ACCOUNTS.

BACKGROUND CONCERNING TWITTER

44. X Corp. owns and operates Twitter, a social networking and microblogging service that can be accessed at http://www.twitter.com and via the Twitter mobile application ("app"). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

45. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called "Tweets," with the public or, alternatively, to "protect" their Tweets by making them viewable by only a preapproved list of "followers." Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets ("retweet") or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

46. Twitter also permits its users to exchange private messages, known as "direct messages" or "DMs," with other Twitter users. DMs, which also may include photos, videos, links, and/or text, can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users. Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter user has the ability to alter the settings on their Twitter account so that they can receive direct messages only from (1) individuals to whom the user has already sent a direct message and (2) Twitter accounts that the user "follows" via his account.

47. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to "follow" accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter's website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique user ID ("UID"). A user must also select a password as well as a unique Twitter username (also known as a "handle"). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the "display name"), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change their password, username, and/or display name at any time, but the UID for the account will remain constant.

48. While anyone can sign up and use Twitter for free, as of November 2021 Twitter also offered a subscription model that offered users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue

at any time. Twitter Blue allows a user to make changes to published tweets, allows users to turn on an "Undo Tweet" feature which keeps a tweet private during a set Tweet Undo period of between 5 and 60 seconds, or until the user taps "Send now," and allows users to Tweet up to 10,000 characters.

49. At the time of Twitter account creation, X Corp. asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. X Corp. also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user's account was created; and (2) the method of account creation (e.g., website or Twitter app).

50. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information including (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify his location, to provide a link to his website, or to specify his date of birth.

51. As noted above, Twitter users can use their account to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing them that they have been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will

receive a notification that someone replied to their message, and the notification will show the content of that reply.

52. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts http://t.co/. Twitter tracks how many times these shortened links are clicked.

53. A registered Twitter user can also "like" a Tweet by clicking a heart icon on a Tweet sent by another user. If another user "likes" a Tweet that is posted by the Twitter user, a notification will appear in the user's account identifying what Tweet was liked and who liked it.

54. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a "media timeline" on their profile that displays "the photos, videos, and GIF's [the accountholder] has uploaded with [their] Tweets." An individual can view a Twitter user's media timeline by visiting the user's Twitter profile page.

55. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access their precise location information, the Twitter user will have the option of attaching their location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter's in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user's choice as well as the device's precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing their location from their Tweets) at any time, and they can delete their past location data from Tweets that have already been sent.

56. A Twitter user may choose to "follow" another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the "follow" button on the other user's Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the "follow" button and waiting for the other user to approve their request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user's Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform them about the new follower. Each user's Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can "unfollow" other users whom they previously followed at any time. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

57. A Twitter user can also "block" other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user's Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks them.

58. A Twitter user can also use Twitter's integrated search function. When a user types a search term into Twitter's search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.

59. A Twitter user can also join or create "Lists" of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List

will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which it may appear.

60. Twitter also offers a functionality called "Spaces," which it calls "a new way to have audio conversations on Twitter." Any user can create a Space; that user is referred to as the "host." Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to their Space and invite them to join. By default, the only individuals permitted to speak in a Space are the individuals that the host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can speak in a Space at a given time.

61. Twitter also offers the ability to sign into third-party apps and websites using one's Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using their Twitter account. Doing so grants the third-party service access to the Twitter user's account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user's Tweets, see who the user follows on Twitter, post Tweets to the user's profile, or access the user's email address. A user can revoke a third-party app or website's authorization to access their Twitter account and associated data at any time.

62. X Corp. collects and retains information about a user's use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user's Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user's account; (4) the content uploaded to a user's profile page, including their avatar, banner image, and bio; (5) information

about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. X Corp. also collects and retains various other data about a user and his/her activity, including:

a. logs of Internet Protocol ("IP") addresses used to login to Twitter and the timestamp associated with such logins;

b. transactional records reflecting, for example, when a user changed their display name or email address;

c. the identities of accounts that are blocked or muted by the user; and

d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

63. In some cases, Twitter users may communicate directly with X Corp. about issues relating to their account, such as technical problems or complaints. Social networking providers like X Corp. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. X Corp. may also suspend a particular user for breaching X. Corp.'s terms of service, during which time the Twitter user will be prevented from using Twitter's services.

64. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other things, the browser being used, its version number, and details about

the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

65. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

66. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

67. In addition, the user's account activity, logs, stored electronic communications, and other data retained by X Corp. can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

68. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

69. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

70. Therefore, X Corp.'s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter possess, distribute, transport, receive, or sell Child Sexual Abuse Material. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

71. Based on the forgoing, I request that the Court issue the proposed search warrant because there is probable cause to believe that evidence of a criminal offense, namely a violations of 18 U.S.C. §2252 and 18 U.S.C. §2252A, is located within Twitter accounts which are more fully described in Attachment A, which is incorporated herin by reference.

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on X Corp.. Because the warrant will be served on X Corp., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with Twitter accounts:

- "@bellamellayella", account #717375314483967;
- "@lexxiisback", account #111100982120124416;
- "@_LoveEndia", account #2755568626;
- "@BiSexUWell", account #1017895112729296896; and
- "@X.aldn", account #1711486293023059968,

(the "Accounts") that are stored at premises owned, maintained, controlled, or operated by X Corp., a company headquartered at 1355 Market Street, Suite 900, San Francisco, CA.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by X Corp.

To the extent that the information described in Attachment A is within the possession, custody, or control of X Corp., regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to X Corp., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 17, 2023 (Case #0348939677), X Corp. is required to disclose to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from June 1, 2021 to present;

7. Privacy and account settings, including change history; and

8. Communications between X. Corp. and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the Account from June 1, 2021 to present, including but not limited to:

1. The content of all Tweets created, drafted, favorited/liked, or retweeted by the Account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the Account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the Account and other Twitter users from June 1, 2021 to present, including but not limited to:

1. All users the Account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the Account;

2. All information from the "Connect" or “Notifications” tab for the account, including all lists of Twitter users who have favorited or retweeted tweets posted by the account, as well as all tweets that include the username associated with the account (i.e., “mentions” or “replies”);

3. All contacts and related sync information; and

4. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the Account, including but not limited to:

1. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the Account;

3. All records of searches performed by the from June 1, 2021 to present;

4. All location information, including all location data collected by any plugins, widgets, or the “Tweet With Location” service, from from June 1, 2021 to present; and

5. All information about the Account's use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the Account was clicked.

X Corp. is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C § 2252(3)(A) and 2252(3)(B) – Knowlingly sell or possess with intent to sell Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1) – Transportation of Child Pornography and 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2) – Possession of Child Pornography, those violations involving Endia Taper and unknown subjects and occurring after June 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The receipt, sale, transportation, or possession on Child Sexual Abuse Material;

(b) Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account owner;

(c) Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic

data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by X Corp., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of X Corp. The attached records consist of _____ [[**GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)**]]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of X Corp., and they were made by X Corp. as a regular practice; and

b. such records were generated by X Corp.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of X Corp. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by X Corp., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date _____ Signature _____